future internet

MDPI

Article

Investigating IPTV Malware in the Wild

Adam Lockett [1], Ioannis Chalkias [2], Cagatay Yucel [1,*], Jane Henriksen-Bulmer [1] and Vasilis Katos [1]

[1] Department of Computing & Informatics, Faculty of Science & Technology, Bournemouth University, Fern Barrow, Wallisdown, Dorset BH12 5BB, UK; s5062305@bournemouth.ac.uk (A.L.); jhenriksenbulmer@bournemouth.ac.uk (J.H.-B.); vkatos@bournemouth.ac.uk (V.K.)
[2] Centre for Research and Technology Hellas, Information Technologies Institute, 570 01 Thessaloniki, Greece; ichalkias@iti.gr
* Correspondence: cyucel@bournemouth.ac.uk

Abstract: Technologies providing copyright-infringing IPTV content are commonly used as an illegal alternative to legal IPTV subscriptions and services, as they usually have lower monetary costs and can be more convenient for users who follow content from different sources. These infringing IPTV technologies may include websites, software, software add-ons, and physical set-top boxes. Due to the free or low cost of illegal IPTV technologies, illicit IPTV content providers will often resort to intrusive advertising, scams, and the distribution of malware to increase their revenue. We developed an automated solution for collecting and analysing malware from illegal IPTV technologies and used it to analyse a sample of illicit IPTV websites, application (app) stores, and software. Our results show that our IPTV Technologies Malware Analysis Framework (IITMAF) classified 32 of the 60 sample URLs tested as malicious compared to running the same test using publicly available online antivirus solutions, which only detected 23 of the 60 sample URLs as malicious. Moreover, the IITMAF also detected malicious URLs and files from 31 of the sample's websites, one of which had reported ransomware behaviour.

Keywords: malware analysis; cyber threat intelligence; IPTV; digital investigations

Citation: Lockett, A.; Chalkias, I.; Yucel, C.; Henriksen-Bulmer, J.; Katos, V. Investigating IPTV Malware in the Wild. *Future Internet* **2023**, *15*, 325. https://doi.org/10.3390/fi15100325

Academic Editor: Claude Chaudet

Received: 28 July 2023
Revised: 18 September 2023
Accepted: 26 September 2023
Published: 28 September 2023

1. Introduction

As many illicit content providers supply copyright-infringing IPTV content for free, they often rely on intrusive advertising, tracking, scams, and malware to make a profit. Illicit content providers also get paid by malware authors to infect their own illicit IPTV websites or software, which are frequently malware families that can generate indirect income with ease, such as cryptocurrency-mining malware [1,2]. One study found that dozens of illicit IPTV websites contained "download now" adverts, redirecting users to landing pages with instructions for downloading malicious browser extensions [3]. Another study found that for the Australian population, 99% of advertisements on illicit content-sharing websites were categorised as high risk, with 46% of these advertisements classified as malicious [4]. Overall, this implies that using copyright-infringing IPTV technologies poses a significant risk to users' devices, as illicit content providers cannot be trusted and may use malware to increase their revenue.

Internet Protocol Television (IPTV) is a service that provides TV programmes and on-demand video content under the TCP/IP internet protocols [5]. Most legal IPTV services supply video content as part of a TV licence, one-time purchase, or paid subscription, whereas free alternatives usually incorporate advertisements. While IPTV services each have many different genres of video content, users often need to subscribe to multiple services to view the specific films and TV programmes they want to watch. Due to the limited effort, convenience, and monetary costs of these legal IPTV services, many users instead choose to use copyright-infringing IPTV technologies to view video content illegally. A report by Sandvine estimates that "roughly 6% of all households in North America

currently have a Kodi device configured to access unlicensed files and streams" [6]. This implies that many IPTV users are willing to risk compromising their home network by installing potentially infected software to access unlicensed video content in addition to possible legal action for copyright infringement.

One of the reasons why infringing IPTV users are willing to risk legal action or exposure to malware and scams is that illegal IPTV services are usually either free or have low monetary costs in comparison to legal IPTV services [7]. Additionally, applications and various software for accessing infringing content can be installed from unofficial software and application stores on physical set-top boxes, which appeals to users due to its ease of use, facilitating a "wide range of illicit content being available in one place, without the need for multiple subscriptions" [8]. Because of the lower perceived costs, these users are willing to accept the risks of trusting and potentially disclosing credit card or personal information to illicit content providers who cannot be trusted and who could be frauds.

The addition of the malware threat to this criminal environment adds another dimension to criminal activities, creating a poly-criminal environment. This was observed in the technical report on the online investigation of IP crime [9], which found that in many cases, the financial gain in one criminal activity supports the other, thus creating a vicious many-folded criminal ecosystem. Another importance in illuminating the malware ecosystem behind illegal IPTV is that it will challenge the judicial process behind the illegal IPTV ecosystem by stressing the fact that the severity of crime increases once the malware is added into the mix.

Our research found that currently, there are insufficient forensic investigation studies and actionable intelligence collections available to effectively identify the risks and threats of malware from using illegal IPTV technologies [10]. This is in part due to an inadequate number of studies and malware analyses that have assessed the likelihood and severity of malware threats in the illegal IPTV ecosystem. An exception is the research that has been conducted for malicious PDF files and fileless threats in the form of malicious JavaScript codes [11]. Features from the embedded PDF files are extracted and utilised for classification. The differentiation of our study with this study is that we have provided an investigation framework, and our classification is based on cyber threat intelligence sources, which depends on the collective work of cyber threat analysts. The novelty of the framework comes within the niche field of IPTV and the recursive collection and query methodology rather than through signature generation over extracted features. Similar malicious URL detection literature can be found in the work of Aljabri et al. [12].

Moreover, malware threats are constantly changing, necessitating malware analyses to be completed consistently on an ongoing basis to provide timely threat intelligence about the risks of infringing IPTV technologies [13–16]. Although there are a small number of indicators of compromise (IOCs) relating to illegal IPTV technologies that exist, such as the AlienVault Open Threat Exchange intelligence platforms, our research shows that there is minimal threat intelligence about the main types of malware used, their severity, and the prominent Tactics, Techniques, and Procedures (TTPs) used by threat actors to exploit the devices of infringing IPTV technology users.

However, in other areas of research, the prevalent malware families, their severity, and the likelihood of infection from using copyright-infringing technologies have been identified. For example, Bosco and Shalaginov, while not focusing specifically on infringing IPTV technology, identified the malware families found in technologies providing copyright-infringing digital content and actionable threat intelligence into the main malware threats from digital content piracy technologies, although these may be less relevant for threat intelligence researchers in the future due to the ever-changing nature of malware threats [17,18].

For example, a security report by Ponemon Institute found that fileless malware [19–21] attacks have been steadily increasing over time, while the number of zero-day attacks nearly doubled between 2019 and 2020 [22]. Additionally, Bosco and Shalaginov found that when searching for popular films in a web browser to identify

illicit IPTV websites, 20% of websites had been removed from the search results and replaced with new sites between two rounds of analysis, with 8% of the websites classified as malicious by VirusTotal [17]. These results suggest that both malware threats and the copyright-infringing IPTV ecosystem are changing continuously. This may be partially due to legal "whack-a-mole" enforcement that removes illicit websites, coupled with the development of zero-day malware to exploit new vulnerabilities. Therefore, to address this issue, in this paper, we present a framework for analysing malware threats in illegal IPTV technologies, the illegal IPTV Technologies Malware Analysis Framework (IITMAF).

The IITMAF has been designed to identify new threats and risks and encourage ongoing evaluation of these. The framework consists of a methodology for securely detecting, collecting, and analysing malware from infringing IPTV technology in addition to identifying and assessing the risks of using these technologies. Moreover, the framework provides a software solution for automating the collection and analysis of malware found in illegal IPTV websites and software, with the focus of the automated software solution being the provision of actionable information.

Actionable information should be relevant, timely, accurate, complete, and ingestible [23]. The IITMAF aims to meet these actionable information requirements for malware in infringing IPTV technologies by providing a solution that can quickly analyse identified URLs for illicit IPTV websites, app stores, and software files using static and dynamic analysis techniques and can consecutively generate a comprehensive report in a structured format. In addition to the identification of malicious URLs and malware analysis capabilities, the framework has also shown to be useful for generating cyber threat intelligence, TTPs, and similar attack patterns, as can be found in the evaluation section. The rest of the paper is structured as follows: Section 2 provides a comprehensive review of the relevant literature on cyber threat intelligence in the IPTV ecosystem and makes the necessary definitions. Section 3 outlines the high-level methodology, including the data collection and data flow diagram of the framework. Section 4 presents and discusses the implementation, the test case, and the evaluation. Section 5 critically evaluates the main findings and their implications, and Section 6 concludes the paper while presenting the limitations.

2. Background

Illegal IPTV technologies consist of physical set-top boxes, websites, or software in the form of standalone applications or illicit add-ons to legal software [7]. Supplying these technologies for use without paying for the content they transmit is a crime. One study identified trojan, adware, spyware, and backdoor malware from content theft websites [17], implying that illicit IPTV providers may include malware in their websites and software or advertise malware disguised as a desirable application to increase their profits. Thus, as illicit IPTV providers are already committing a crime, it appears that, in addition, many of these providers elect to distribute malware as part of the delivery to supplement their income. The following sections will define the illegal IPTV technologies used and their risks in addition to outlining relevant malware collection and analysis techniques for these technologies.

Illicit Streaming Devices (ISDs) are physical boxes or USB sticks that connect to a TV to provide free television and film content that you would usually pay to view [8]. Many physical IPTV boxes, such as Kodi boxes, are legal, but third-party software can be installed to illegally stream IPTV content for free. Conversely, other physical IPTV boxes, often described as "fully loaded" or "jailbroken", already include software for facilitating illegal IPTV streaming. Because ISD providers are already willing to commit copyright infringement, they are more likely to commit further breaches of law, as it could increase their profits. Therefore, ISD providers cannot be trusted, as they could supply users with ISDs infected with malware.

Overall, ISD providers are unlikely to infect the products they sell with high-impact malware when they are already making a profit from selling ISDs. However, potential

users would likely purchase an ISD from a website, which itself could be a scam designed to try and get individuals to disclose their credit card details. Moreover, fake websites that advertise illegal IPTV boxes could also distribute fileless malware when visited by users. Therefore, there are other risks to purchasing and using ISDs, as the providers cannot be trusted and could be attempting to scam people.

Websites for streaming IPTV content illegally are available over the surface web, with examples including PutLocker and FlixTor. IPTV content is usually freely available on these websites, which is attractive to users who are not willing to pay for a streaming service or risk purchasing an ISD. However, as the illicit content provided is often free, IPTV websites are untrustworthy, as they are more likely to rely on trackers, scams, and malware to gain a profitable income.

Illegal IPTV websites have different strategies for providing infringing IPTV content. Many sites host and potentially live-stream IPTV content on their website, although these websites are more likely to be detected by anti-piracy organisations. To reduce the risk of legal action, some websites collect and contain lists of hyperlinks to websites for accessing IPTV content illegally, known as "link aggregators" [9]. Link aggregators can also be found on legitimate websites, such as GitHub repositories and forum posts.

Once more, using illegal IPTV websites or aggregators is risky, as they cannot be trusted. In comparison to ISDs, IPTV websites are potentially riskier because they receive no income for providing free IPTV content, whereas ISDs are purchased. Hence, IPTV websites rely on intrusive advertising and malware to gain a profit, with adverts often redirecting users to malicious or scam websites when clicked on [7]. This is known as malvertising (malicious advertising), which distributes malware by injecting online advertisements with malicious code [24]. Cybersecurity company RiskIQ found that 1 in 3 content theft websites expose visitors to malware, with hackers paying the providers USD 70 million to add malware to their websites [1]. This implies there is a significant chance of users obtaining infected with high-severity malware, especially if hackers are willing to pay a total of USD 70 million.

Malware can be distributed to users of illegal IPTV websites when users download video files for watching IPTV content, such as MP4 files. When an infected file is opened, the malware will execute on the user's device, which could be anything from ransomware to a remote access trojan (RAT). Although users may not realise the risks of downloading files from an untrustworthy source, technically proficient users will be aware of the risks and are likely to mitigate the risk of infecting their devices by using an antivirus that scans files or a virtual machine (VM).

However, this is not the only risk of using IPTV websites. Another risk is fileless malware. Fileless malware does not require a user to download a malicious file; rather, it exploits vulnerable applications on a victim's device to enable the injection of malicious code into its main memory [25]. Fileless malware is a high risk to users, as it is unlikely to be detected by antivirus signatures and could potentially infect a user as soon as they visit a website [26].

One study analysed the malicious codes in embedded PDFs. Moreover, malicious codes embedded into the PDF files present a prevalent way of infecting the main memory and using malicious JavaScript codes [11]. There are several recent data-dependent malicious URL identification and classification studies in the literature based on machine learning, deep learning, or an ensemble of classification algorithms [12,27–31]. Furthermore, considering the methodology, our paper shows similarity in the collection of cyber threat intelligence with the works of Ghaleb et al. [30] and by the similarity of analysing the websites within a framework with the works of Rafsanjani et al. [31]. However, our paper differentiates from the literature by providing an exemplar analysis for the niche domain of illicit IPTV websites' identification of malvertising and providing the tools and best practices that frame the investigation guideline.

Furthermore, many threat intelligence platforms, such as VirusTotal and AlienVault Open Threat Exchange (OTX), do not recognise these sites as malicious. To illustrate, we

scanned 1555 illicit IPTV websites and aggregators gained from an IPTV GitHub repository in VirusTotal. Of these websites, only 34 were identified as malicious or had an association with malware for both VirusTotal and AlienVault OTX even though many of these websites contained intrusive advertisements attempting to scam users into downloading potentially unwanted programs (PUPs) that may have been malicious.

Infringing IPTV (Pro v7.0.6) software includes standalone desktop and mobile phone applications in addition to add-ons or plugins for legitimate IPTV software, such as Kodi. Using standalone applications to access IPTV content illegally often requires paid subscriptions. A study found that a business, SET TV, offered infringing IPTV content to over 180,000 users with a USD 20 monthly or USD 200 annual subscription via a standalone software application [7]. Again, it is less likely that providers will infect IPTV applications with malware if they are already making a profit. In comparison to using websites for IPTV, there is more incentive for IPTV website providers to include malware, as the content provided is usually free. However, downloading and executing an application infected with malware could have a greater impact if users do not have antivirus software installed.

While studies suggest that standalone infringing IPTV applications have a considerable number of users, another study found that 26 million Kodi users (68% of the total user base) were pirating illegal IPTV content using Kodi (20.2) software add-ons [32]. Although these add-ons are often downloaded from likely benign GitHub repositories, the Digital Citizens Alliance found that third-party Kodi add-ons were used to distribute cryptocurrency-mining malware [2]. Similarly, Warrior et al. found that 1.4% of Kodi add-ons resolved to domain IP addresses found on malicious blacklists (131 out of 9146 add-ons studied) [10]. This implies that add-ons facilitating the streaming of illicit IPTV content are more widely used than standalone applications and may be more likely to be infected with malware.

3. Implementation

Requirements for the framework were elicited through secondary research of the existing literature on the topics of malware forensics and the illegal IPTV ecosystem, which enabled the gathering of requirements for the collection and analysis of malware from illegal IPTV technologies. Exploratory research consisting of analysing a sample of 1555 illicit IPTV websites in AlienVault OTX and VirusTotal was also completed to obtain the requirements. The research results allowed the identification of the types of malwares in illicit IPTV websites, determining the approaches for detecting and collecting malware from these websites and establishing the methodology and best practices of the framework for collecting and analysing a dataset of illegal IPTV technologies.

Figures 1 and 2 present the overall methodology and a high-level data flow diagram, respectively. The software solution has a client-server structure with an API "dispatcher" server to handle requests from a "requester" client. This can enable multiple users with requester clients to issue requests to the dispatcher, providing scalability.

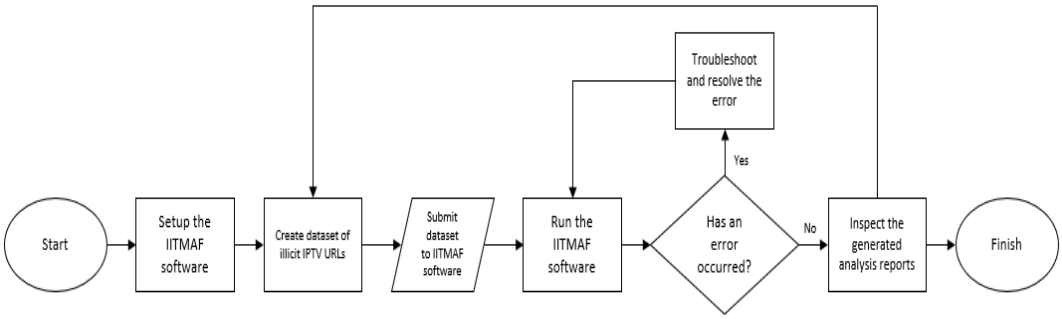


Figure 1. Flow chart of the framework's automated malware collection and analysis methodology.

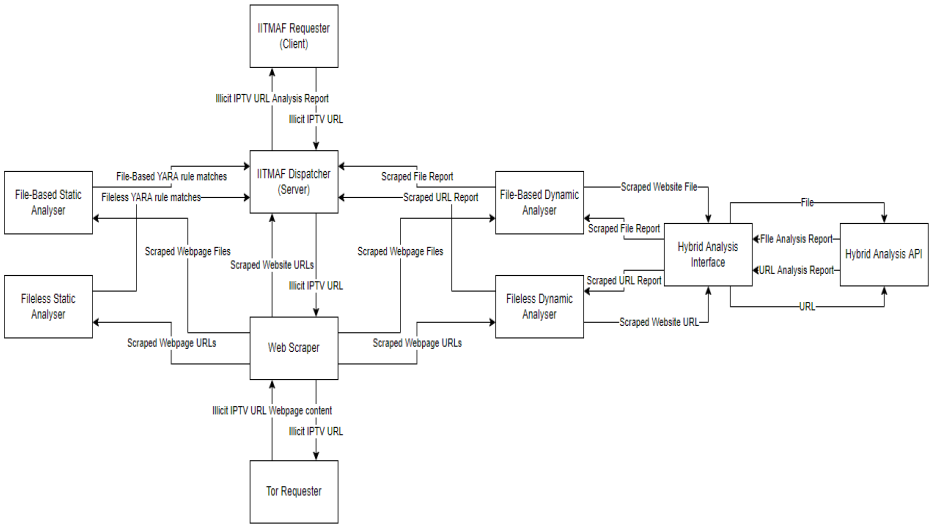


Figure 2. DFD design of the IITMAF software solution.

The IITMAF consists of several components working together to support the investigations for the IPTV ecosystem. A web scraper was designed and implemented for the collection of malicious scripts and files. A Tor requester was implemented in the scraper so that the anonymity of the investigator was ensured. For the collected artefacts, both file-based and fileless static analysers were included in the framework since, as explained previously, malicious actions and objectives are sometimes provided within a shellcode/script format. In Figure 2 below, a detailed data flow diagram of how these modules interact with each other is given.

The development environment of the IITMAF's automated software solution consisted of a Windows 10 PC with Python 3.8.6 installed. Visual Studio Code was selected for the IDE, as it supports Python and integrates with GitHub. Moreover, Tor was installed and configured to run as a Windows service to enable the IITMAF software solution to make anonymous HTTP requests.

The dispatcher (see Figure 2) provides a REST API that enables the collection and analysis of malware from illegal IPTV technologies. It serves several API endpoints that are called by the requester client to submit URLs. While the API is currently configured to run locally, it can be configured to make the API accessible over the internet, enabling any cybersecurity professional to identify and analyse malware in the illegal IPTV ecosystem. Additionally, the API endpoints can be accessed using Curl, Postman, or any programming language that can initiate and handle HTTP endpoints, potentially allowing organisations, such as intellectual property offices, to use the IITMAF as a threat feed for providing cyber threat intelligence.

The dispatcher has four endpoints, consisting of endpoints for scraping URLs from a webpage; iteratively scraping URLs from a website; static analysis; and dynamic analysis. The requester client is used to submit the dataset of illicit IPTV URLs to the dispatcher API server sequentially and process the results to generate a report for each URL submitted. This allows multiple URLs to be submitted to the API and be analysed without having to manually submit every URL.

3.1. Malware Collection and Analysis

For the malware analysis functions, file and webpage URLs are collected from a given webpage URL using a website scraper, which is then added to a list and queued for analysis, with the given webpage's URL and domain appended to the front of this list as shown in Figure 3. If a URL pointing to a non-webpage file is submitted, the webpage scraper collects URLs and files from the URL path with the filename removed instead, which will include the original URL submitted.

Figure 3. Dispatcher console showing files being downloaded from an illicit IPTV website.

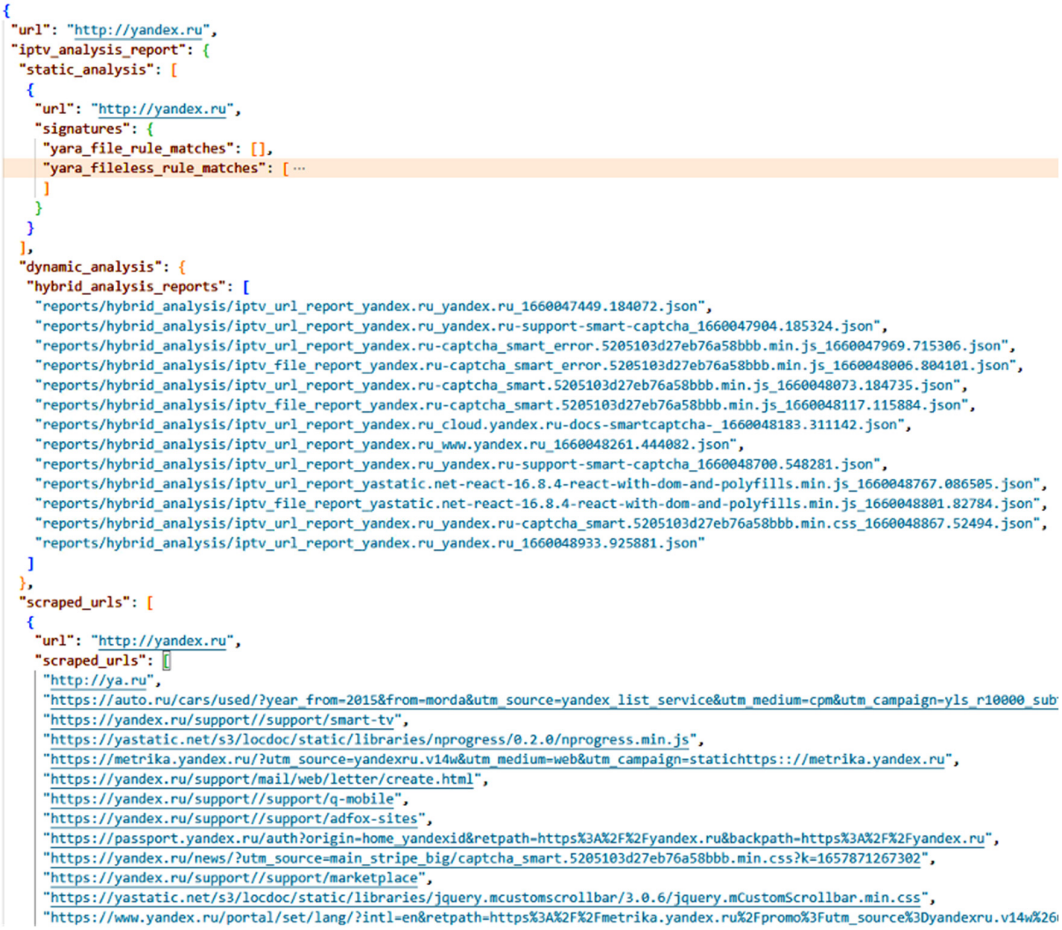
Once the URLs have been collected, they are queued for either file-based or fileless static analysis. If a URL contains a webpage file type or no file type, it is submitted to static fileless analysis. Otherwise, URLs are submitted to file-based static analysis with the files downloaded first.

The URLs and downloaded files are then compared with either file-based malware or fileless malware YARA rules, identifying any binary or textual patterns that indicate a file or webpage has malicious capabilities. Any YARA rule matches for a URL or file are then recorded and stored as a JSON object to be used in the generated report. When the static analysis process is complete, the collected URLs are submitted to either file-based or fileless dynamic analysis, similar to the static analysis process. However, JavaScript (JS) files are submitted to both file-based and fileless dynamic analysis, as JS files can contain malware, and hence, analysing JS files in different environments could provide more accurate results.

The dynamic analysis entails submitting the collected URLs and files to an isolated sandbox environment for automated analysis using the Hybrid Analysis API (https://www.hybrid-analysis.com/ (accessed 25 August 2023)) with a generated analysis report returned once the analysis is complete.

3.2. Report Generation

When all the collected files and URLs have been analysed, a single report is generated for each URL submitted to the dataset text file. Each report contains a section for the URLs retrieved from the iterative URL collection function, static analysis results, and dynamic analysis report file paths. The report only contains the file paths of the Hybrid Analysis reports generated from the dynamic analysis or else the report would be too large. Figure 4 displays a sample of a generated analysis report and shows the dynamic analysis reports generated and the URLs scraped from the given URL webpage.



```
{
 "url": "http://yandex.ru",
 "iptv_analysis_report": {
  "static_analysis": [
   {
    "url": "http://yandex.ru",
    "signatures": {
     "yara_file_rule_matches": [],
     "yara_fileless_rule_matches": [ ···
     ]
    }
   }
  ],
  "dynamic_analysis": {
   "hybrid_analysis_reports": [
    "reports/hybrid_analysis/iptv_url_report_yandex.ru_yandex.ru_1660047449.184072.json",
    "reports/hybrid_analysis/iptv_url_report_yandex.ru_yandex.ru-support-smart-captcha_1660047904.185324.json",
    "reports/hybrid_analysis/iptv_url_report_yandex.ru-captcha_smart_error.5205103d27eb76a58bbb.min.js_1660047969.715306.json",
    "reports/hybrid_analysis/iptv_file_report_yandex.ru-captcha_smart_error.5205103d27eb76a58bbb.min.js_1660048006.804101.json",
    "reports/hybrid_analysis/iptv_url_report_yandex.ru-captcha_smart.5205103d27eb76a58bbb.min.js_1660048073.184735.json",
    "reports/hybrid_analysis/iptv_file_report_yandex.ru-captcha_smart.5205103d27eb76a58bbb.min.js_1660048117.115884.json",
    "reports/hybrid_analysis/iptv_url_report_yandex.ru_cloud.yandex.ru-docs-smartcaptcha-_1660048183.311142.json",
    "reports/hybrid_analysis/iptv_url_report_yandex.ru_www.yandex.ru_1660048261.444082.json",
    "reports/hybrid_analysis/iptv_url_report_yandex.ru_yandex.ru-support-smart-captcha_1660048700.548281.json",
    "reports/hybrid_analysis/iptv_url_report_yastatic.net-react-16.8.4-react-with-dom-and-polyfills.min.js_1660048767.086505.json",
    "reports/hybrid_analysis/iptv_file_report_yastatic.net-react-16.8.4-react-with-dom-and-polyfills.min.js_1660048801.82784.json",
    "reports/hybrid_analysis/iptv_url_report_yandex.ru_yandex.ru-captcha_smart.5205103d27eb76a58bbb.min.css_1660048867.52494.json",
    "reports/hybrid_analysis/iptv_url_report_yandex.ru_yandex.ru_1660048933.925881.json"
   ]
  },
  "scraped_urls": [
   {
    "url": "http://yandex.ru",
    "scraped_urls": [
     "http://ya.ru",
     "https://auto.ru/cars/used/?year_from=2015&from=morda&utm_source=yandex_list_service&utm_medium=cpm&utm_campaign=yls_r10000_sub
     "https://yandex.ru/support//support/smart-tv",
     "https://yastatic.net/s3/locdoc/static/libraries/nprogress/0.2.0/nprogress.min.js",
     "https://metrika.yandex.ru/?utm_source=yandexru.v14w&utm_medium=web&utm_campaign=statichttps:://metrika.yandex.ru",
     "https://yandex.ru/support/mail/web/letter/create.html",
     "https://yandex.ru/support//support/q-mobile",
     "https://yandex.ru/support//support/adfox-sites",
     "https://passport.yandex.ru/auth?origin=home_yandexid&retpath=https%3A%2F%2Fyandex.ru&backpath=https%3A%2F%2Fyandex.ru",
     "https://yandex.ru/news/?utm_source=main_stripe_big/captcha_smart.5205103d27eb76a58bbb.min.css?k=1657871267302",
     "https://yandex.ru/support//support/marketplace",
     "https://yastatic.net/s3/locdoc/static/libraries/jquery.mcustomscrollbar/3.0.6/jquery.mCustomScrollbar.min.css",
     "https://www.yandex.ru/portal/set/lang/?intl=en&retpath=https%3A%2F%2Fmetrika.yandex.ru%2Fpromo%3Futm_source%3Dyandexru.v14w%26
```


Figure 4. Sample generated analysis report.

3.3. Evaluation

To evaluate the IITMAF and showcase the main features of the IITMAF's automated software solution, we trialled the software on an illicit IPTV website, zmovies.co, applying the automated methodology of the framework outlined in Section 3.1.

Before submitting the URL of zmovies.co to the dataset and running the IITMAF software solution, we made some modifications to the solution configuration file. The configuration file enables the user to set limits to the collection and analysis to shorten the duration of a dataset's analysis or to increase the volume of information reported. We set the scraper depth to 3, the maximum number of URLs scraped to 300, and the dynamic analysis submission limit to 25, as shown in Figure 5.

```
[Triage]
TRIAGEURL = https://api.tria.ge/v0/
TRIAGEKEY = <KEY>

[HybridAnalysis]
HYBRIDANALYSISKEY = <KEY>
HYBRIDANALYSISURL = https://www.hybrid-analysis.com/api/v2/

[IterativeURLScraping]
ITERATION_DEPTH = 3
SCRAPED_URLS_LIMIT = 300

[Analysis]
DYNAMIC_ANALYSIS_SUBMISSIONS_LIMIT = 25
```

Figure 5. Configuration file of the IITMAF software solution.

Once the configuration was complete, the dispatcher API and requester client of the IITMAF software solution were executed, initiating the iterative URL collection as shown in Figure 6.

```
Iteration scanner depth: 1
URLs scraped: 87
URLs scraped: 106
URLs scraped: 125
URLs scraped: 144
URLs scraped: 146
URLs scraped: 165
URLs scraped: 184
URLs scraped: 203
URLs scraped: 205
URLs scraped: 207
Iteration scanner depth: 2
URLs scraped: 305
URLs extracted from website: 87
127.0.0.1 - - [10/Aug/2022 12:52:22] "GET /api/v1/website/urls HTTP/1.1" 200 -
URLs extracted from webpage: 20
http://zmovies.co/favicon-16x16.png
 favicon-16x16.png
http://zmovies.co/apple-touch-icon.png
 apple-touch-icon.png
http://zmovies.co/site.webmanifest
 site.webmanifest
http://zmovies.co/favicon-32x32.png
 favicon-32x32.png
```

Figure 6. Dispatcher console showing the iterative URL collection functionality.

The iterative URL collection function extracted 87 unique URLs from the given website URL with any duplicate URLs removed from the list, while 20 URLs were extracted from the webpage of the given URL and queued for analysis.

For the analysis, any URLs pointing to files were downloaded, with some of the files downloaded shown in Figure 7. Once the static and dynamic analysis was complete, a report was generated, with a sample of the report presented in Figure 7.


```
"dynamic_analysis": {
 "hybrid_analysis_reports": [
  "reports/hybrid_analysis/iptv_url_report_zmovies.co_zmovies.co_1660132449.702171.json",
  "reports/hybrid_analysis/iptv_url_report_zmovies.co_www.sav.com-shopping-premium_domain_checkout_step_one_1660132516.693384.json",
  "reports/hybrid_analysis/iptv_url_report_zmovies.co_cdnjs.cloudflare.com-ajax-libs-font-awesome-5.9.0-css-all.css_1660132582.432543.json",
  "reports/hybrid_analysis/iptv_file_report_zmovies.co-favicon-16x16.png_1660132615.544393.json",
  "reports/hybrid_analysis/iptv_url_report_zmovies.co_zmovies.co-css-for_sale_lander.css_1660133073.471183.json",
  "reports/hybrid_analysis/iptv_url_report_zmovies.co_zmovies.co_1660133152.320829.json",
  "reports/hybrid_analysis/iptv_url_report_zmovies.co_www.sav.com-pages-terms_toc_1660133658.182615.json",
  "reports/hybrid_analysis/iptv_url_report_cdnjs.cloudflare.com-ajax-libs-FitText.js-1.2.0-jquery.fittext.min.js_1660133726.073212.json",
  "reports/hybrid_analysis/iptv_file_report_cdnjs.cloudflare.com-ajax-libs-FitText.js-1.2.0-jquery.fittext.min.js_1660133987.197082.json",
  "reports/hybrid_analysis/iptv_url_report_zmovies.co_www.sav.com-domains-sell_1660134427.93187.json",
  "reports/hybrid_analysis/iptv_url_report_zmovies.co_stackpath.bootstrapcdn.com-bootstrap-4.2.1-css-bootstrap.min.css_1660134852.769351.json",
  "reports/hybrid_analysis/iptv_url_report_zmovies.co_www.sav.com-pages-contact_1660135294.964748.json",
  "reports/hybrid_analysis/iptv_file_report_zmovies.co-apple-touch-icon.png_1660135330.701589.json",
  "reports/hybrid_analysis/iptv_url_report_kit.fontawesome.com-ef48a658a5.js_1660135785.980337.json",
  "reports/hybrid_analysis/iptv_file_report_kit.fontawesome.com-ef48a658a5.js_1660136075.262285.json",
  "reports/hybrid_analysis/iptv_url_report_stackpath.bootstrapcdn.com-bootstrap-4.2.1-js-bootstrap.min.js_1660136516.763663.json",
  "reports/hybrid_analysis/iptv_file_report_stackpath.bootstrapcdn.com-bootstrap-4.2.1-js-bootstrap.min.js_1660136859.113873.json",
  "reports/hybrid_analysis/iptv_url_report_zmovies.co_www.sav.com_1660137367.739496.json",
  "reports/hybrid_analysis/iptv_file_report_zmovies.co-site.webmanifest_1660137400.638286.json",
  "reports/hybrid_analysis/iptv_file_report_zmovies.co-favicon-32x32.png_1660137433.388144.json",
  "reports/hybrid_analysis/iptv_url_report_cdnjs.cloudflare.com-ajax-libs-popper.js-1.14.6-umd-popper.min.js_1660137498.728081.json",
  "reports/hybrid_analysis/iptv_file_report_cdnjs.cloudflare.com-ajax-libs-popper.js-1.14.6-umd-popper.min.js_1660137811.297161.json",
  "reports/hybrid_analysis/iptv_url_report_zmovies.co--widget.trustpilot.com-bootstrap-v5-tp.widget.bootstrap.min.js_1660137886.380603.json",
  "reports/hybrid_analysis/iptv_file_report_zmovies.co--widget.trustpilot.com-bootstrap-v5-tp.widget.bootstrap.min.js_1660137919.039292.json",
  "reports/hybrid_analysis/iptv_url_report_zmovies.co_zmovies.co_1660137999.595023.json"
 ]
},
"scraped_urls": [
 {
  "url": "http://zmovies.co",
  "scraped_urls": [
   "http://zmovies.co#/apple-touch-icon.png",
   "http://zmovies.co#/apple-touch-icon.png/favicon-32x32.png/css/for_sale_lander.css?1660132342",
   "http://zmovies.co#/favicon-16x16.png/site.webmanifest",
   "http://www.sav.com?utm_source=parked_page&utm_medium=click&utm_campaign=premium_domain/cdn-cgi/styles/cf-errors.css",
   "http://zmovies.co#/favicon-32x32.png",
   "http://zmovies.co##/site.webmanifest",
   "https://cdnjs.cloudflare.com/ajax/libs/FitText.js/1.2.0/jquery.fittext.min.js",
   "https://www.cloudflare.com/cdn-cgi/styles/cf.errors.css",
   "http://zmovies.co#/favicon-16x16.png/apple-touch-icon.png",
   "http://www.sav.com?utm_source=parked_page&utm_medium=click&utm_campaign=premium_domain/cdn-cgi/styles/cf-errors.css/cdn-cgi/styles/cf-errors.css",
   "http://zmovies.co#/apple-touch-icon.png/favicon-16x16.png",
   "http://zmovies.co#/favicon-32x32.png/favicon-32x32.png",
   "http://zmovies.co#/apple-touch-icon.png/favicon-32x32.png//widget.trustpilot.com/bootstrap/v5/tp.widget.bootstrap.min.js",
   "http://zmovies.co#//widget.trustpilot.com/bootstrap/v5/tp.widget.bootstrap.min.js/site.webmanifest",
   "http://zmovies.co##/favicon-32x32.png",
```


Figure 7. Sample analysis report showing dynamic analysis and iterative URL collection results.

Although the submitted URL and its scraped files and URLs returned no YARA rule matches, the iterative URL collection and dynamic analysis functions supplied a high number of results, with Figure 7 showing some of the URLs scraped from the given website and the Hybrid Analysis reports generated.

To determine if zmovies.co was associated with malware or malicious activity, we submitted some of the internal and external URLs collected from the website to VirusTotal and checked the generated Hybrid Analysis reports for malicious indicators. While we found a few malicious indicators from the URLs collected, the Hybrid Analysis report of a file scraped from zmovies.co indicated malicious activity.

Figure 8 shows the Hybrid Analysis report for a JavaScript file downloaded from zmovies.co that marks the file as "suspicious" and classifies it as a Trojan HTML Agent.


```
],
"job_id": "62f37faf87f0244aee492086",
"environment_id": 120,
"environment_description": "Windows 7 64 bit",
"size": 153,
"type": "HTML document, ASCII text, with CRLF line terminators",
"type_short": [
 "script",
 "javascript"
],
"target_url": null,
"state": "SUCCESS",
"error_type": null,
"error_origin": null,
"submit_name": "tp.widget.bootstrap.min.js",
"md5": "a1ed5ecb9c651451520019b3747a06ef",
"sha1": "724e59314a0890297915c1010e38e3267cdd810e",
"sha256": "1b47c0dc50d20d7239392e8e3917cf1340aa2acf53b7e6a84ee56714471e26f4",
"sha512": "c9cfa80a019911ce4f3b34d62d5b92db61bb1e51a2bd4a7b6aafb503a367cd594a44d10e9dc9cd97965a2519502c6ec273f1ad66f1e07de7a796f777d86c6fe6",
"ssdeep": "3:qVoB3tURObOb0qHXboAcMBXqWrKb0GklIVLLPj0awcWWGu:q43tIkObRHXiMIWObtklI5LPjLpfGu",
"imphash": "Unknown",
"av_detect": 1,
"vx_family": "Trojan.Html.Agent",
"url_analysis": false,
"analysis_start_time": "2022-08-10T09:57:42+00:00",
"threat_score": 35,
"interesting": false,
"threat_level": 1,
"verdict": "suspicious",
"certificates": [],
"domains": [],
"compromised_hosts": [],
"hosts": [],
"total_network_connections": 0,
"total_processes": 1,
"total_signatures": 9,
"extracted_files": [],
"file_metadata": null,
"processes": [
 {
```


Figure 8. Sample of a Hybrid Analysis report showing the analysis results for a scraped file.

To obtain further information about whether the collected JS file was malicious, we checked the SHA-256 hash of the file in VirusTotal ((*1b47c0dc50d20d7239392e8e3917cf1340aa2acf53b7e6a84ee56714471e26f4*, accessed on 25 August 2023) [3] https://www.virustotal.com/gui/domain/bmovies.vip/relations (*499df4b49ada07ff706a56bc1bf8483f8f78940b4047926d91bc349786bef920*, accessed 25 August 2023) [4] https://www.virustotal.com/gui/url/499df4b49ada07ff706a56bc1bf8483f8f78940b4047926d91bc349786bef920/detection (accessed 25 August 2023)). While only one antivirus tool detected the file as malicious, the relations ([3] and [4]) show that the collected file is often created by known malware files when they are executed.

In conclusion, the IITMAF software solution was able to detect a potentially malicious file collected from an illicit IPTV website and classify it. This shows that the framework can collect URLs and files from illicit IPTV websites and identify malicious activity.

4. Findings

This experiment completed for evaluating the IITMAF entailed submitting a research sample of illegal IPTV technology URLs to the IITMAF and comparing the analysis results with results from VirusTotal. The research sample had a total of 60 URLs consisting of 35 illicit IPTV website URLs, 13 app store URLs (from 7 app stores), and 12 standalone software executable and add-on URLs. Less illicit IPTV app store and software URLs were included in the research sample, as they were more difficult to locate in comparison to websites, which are more accessible using search engines.

For this evaluation (Section 3.3), each sample URL submitted to the IITMAF collected up to 25 URLs, which were then submitted for analysis in addition to the research sample URL. Once the analysis reports had been generated for the research sample, the number of URLs in the research sample identified as malicious was recorded and compared with the results of the research sample URLs submitted to VirusTotal (Table 1). Moreover, the number of URLs in the research sample that scraped URLs or files identified as malicious by the IITMAF was recorded. These results were then compared with the number of URLs in the research sample that identified malicious-related files from 2022 for the domain of the URLs in VirusTotal. Only malicious files from 2022 were used to determine the number of malicious relations for a URL, as VirusTotal is a community-based threat intelligence platform that identifies malware previously submitted that may not be relevant to URLs in 2022. Hence, only recent malware from 2022 was counted.

Table 1. Experiment results of malicious illicit IPTV URLs and files.

IPTV Technology	**IPTV Website**		**IPTV App Store**		**IPTV Software Executable**	
Research sample size	35		13		12	
Solution	IITMAF	VirusTotal	IITMAF	VirusTotal	IITMAF	VirusTotal
Files or URLs identified as malicious in the research sample	27	10	1	6	4	7
Related files or URLs extracted from the research sample URLs identified as malicious	20	12	3 (out of 7 different app store domains)	5 (out of 7 different app store domains)	8	6

Table 1 presents the findings of the experiment completed to evaluate the IITMAF software solution, which was conducted from the 8th to the 16th of August 2022. As VirusTotal identifies related malicious files with a URL domain, we used the domains of the URLs in the research sample to determine whether a URL had related malicious files. Therefore, the related malicious file results for app stores are out of seven, as the thirteen app store URLs in the research sample only include seven different domains.

The experiment results show that the IITMAF solution detected more URLs as malicious than VirusTotal overall, with the IITMAF identifying 32 out of the 60 URLs of the research sample as malicious, while VirusTotal only identified 23 as malicious. Additionally, the IITMAF solution detected related malicious files or URLs for 31 of the research sample URLs, whereas VirusTotal identified 26 malicious relations from 2022.

5. Discussion

Although the IITMAF identified more illicit IPTV technologies as malicious than VirusTotal, VirusTotal classified a greater number of illicit IPTV app store and software URLs as malicious than the IITMAF. This is because the app store and software URLs often pointed to Android APK files or had relations with these files, which the dynamic analysis feature of the IITMAF solution is unable to execute and analyse, as it uses a Windows sandbox environment by default. Conversely, the IITMAF was still able to identify 12 of the 25 app store and software URLs as suspicious, and thus, only 8 out of 25 were classified as benign. Moreover, the IITMAF identified ransomware TTPs for three files scraped from an illicit IPTV app store included in the research sample. This demonstrates that the IITMAF is still capable of providing actionable information for a range of illegal IPTV technologies even if it has limitations when analysing APK files. Finally, the IITMAF primarily focuses on the analysis of illicit IPTV websites and the extraction of files and URLs from them. Hence, due to time constraints, the dynamic analysis of Android files that require a different sandbox environment was not implemented.

Figure 9 shows some of these collected URLs for an illicit IPTV website (moviesjoy.to) that includes URLs with external domains potentially used for malvertising. The VirusTotal report for one of the external domains collected for this IPTV website, namely "static.zdassets.com", identified many recent malicious related files that had file names used in intrusive advertisements, which is common in illicit IPTV websites, such as "AntiVirusExe.exe" and "PCCleaner" (https://www.virustotal.com/gui/domain/static.zdassets.com/relations (accessed on 25 August 2023)). Moreover, another URL to an external domain, bigcache.ml, had a URL path pointing to an alleged JQuery library JavaScript file. The VirusTotal report of this URL reported two malicious and one suspicious antivirus alert in addition to classifying the domain as a malware site. This implies that the iterative URL collection function is effective at collecting URLs from a website including any external domains that could be used for malvertising. Hence, the IITMAF is capable of iteratively scraping potentially malicious URLs from a website.

Figure 9. IITMAF report showing collected URLs for one of the illicit webpages.

Thus, this demonstrates that the webpage URL collection function is effective at collecting files and URLs from a webpage and submitting them for analysis. Conversely, a limitation of both the URL collection functions is that website CAPTCHA security mech-

anisms are often triggered when scraping a website, limiting the number of URLs and files that are collected. The likelihood of a CAPTCHA mechanism triggering is increased further where the HTTP requests made by the URL collection functions are routed through Tor. While disabling Tor for the URL collection functions could enable more URLs to be collected, this would make the IITMAF host's public IP address visible to potentially malicious websites, posing a security risk. For this aim, if the Tor function needs to be disabled, it is required to limit the functionality to URL collection. The results of this experiment suggest that the URL collection functions are sufficient even with this limitation in place.

Table 2 shows the correlation from CTI sources collected for all the IPTV websites investigated in this research (Section 4). The table includes details of the following fields:

- Signatures: potentially malicious behavioural/static signatures raised by Hybrid analysis.
- Number of Files: the number of files that are extracted from a webpage.
- Number of Compromised Hosts: from all the URLs that are linking out from this webpage, the number of them that are marked malicious.
- Maximum Threat Score: a metric calculated by Hybrid Analysis (Hybrid Analysis 2022) demonstrating the threat score of a link.
- Malicious File and Fileless Signatures: the number of alerts raised by the crafted YARA rules analysis for file malware or fileless malware signatures, respectively.
- Extracted URLs: the number of URLs that are extracted from a webpage.

Table 2. Correlation matrix of the investigated IPTV webpages.

	Signatures	**Number of Files**	**Number of Compromised Hosts**	**Maximum Threat Score**	**Malicious File Signatures**	**Malicious Fileless Signatures**	**Extracted URLs**
Signatures	1						
Number of Files	0.94	1					
Number of Compromised Hosts	0.34	0.31	1				
Maximum Threat Score	−0.01	0.1	0.47	1			
Malicious file signatures	0.49	0.52	0.2	0.01	1		
Malicious Fileless Signatures	0.59	0.57	0.24	0.01	0.37	1	
Extracted URLs	0.64	0.58	0.29	−0.07	0.48	0.67	1

Thus, Table 2 shows that the signature and number of files that a webpage tries to download highly correlate with the visitor's signatures (value 0.94). Further, a correlation of ~0.67 was observed between the number of fileless signatures and the extracted URLs. This latter correlation can be explained in the form of the delivery of fileless threats, which is the general case through browser exploitations.

For the attribution of malicious threats, the contemporary approach is the identification of the techniques and tactics. This, in return, reveals the modus operandi of the attacker and renders the attribution possible [33]. Therefore, within our experiment, we have also collected the Techniques, Tactics, and Procedures of the MITRE ATT and CK framework and presented below the most common techniques that have been utilised on these IPTV sources:

- T1518: Software Discovery;
- T1082: System Information Discovery;

- T1012: Query Registry;
- T1218.011: System Binary Proxy Execution;
- T1179 also moved to T1056.004: Input Capture: Credential API Hooking;
- T1035: System Services: Service Execution;
- T1518.001: Security Software Discovery;
- T1218.011: RunDLL;
- T1573: Encrypted Channel;
- T1059.007: Command and Scripting Interpreter: JavaScript;
- T1112: Modify Registry.

The breakdown of the use of these techniques can be found in Figure 10.

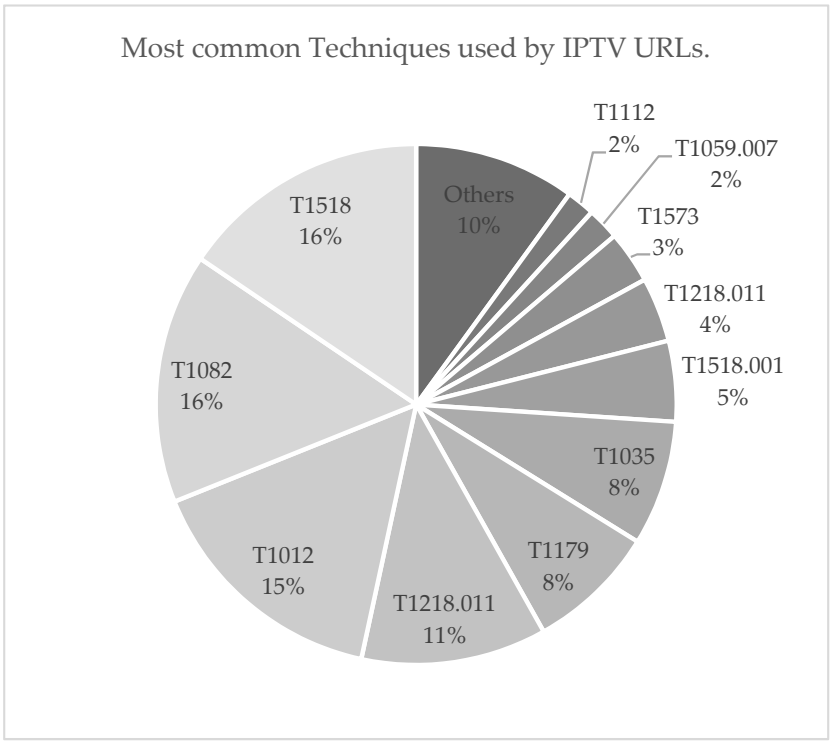


Figure 10. Pie chart for the most common ATT and CK techniques observed.

6. Conclusions

This paper presented the IITMAF, an effective tool for automatically detecting, collecting, and analysing malware from illegal IPTV technologies. We evaluated the framework through a series of use cases and collections where we demonstrated the effectiveness of the IITMAF and showcased the results that can be achieved using the IITMAF when compared to existing solutions. The evaluation results show that the IITMAF is more effective at detecting malicious capabilities and behaviour from illicit IPTV technologies overall, while VirusTotal is more effective at detecting malware from illicit IPTV app stores and software files.

Although VirusTotal identified a greater volume of app store and software URLs as malicious, the IITMAF was intended primarily for analysing illicit IPTV websites, with its iterative URL collection results capable of identifying possible external malvertising domains for an illicit website.

Moreover, the IITMAF produces a more comprehensive analysis report than other solutions, with matched YARA (the pattern-matching tool for malware) rules and dynamic analysis results classifying malware and supplying related TTPs. From the findings (Section 4), the YARA rules detected malicious capabilities in an executable file relating to privilege escalation and a malicious document format. Likewise, the behavioural analysis results of an HTML webpage classified the detected malicious behaviour as an indicator of

ransomware. This demonstrates that the IITMAF can supply actionable threat intelligence for malware detected in the illicit IPTV ecosystem.

Limitations and Future Work

While the experiment results imply that the IITMAF is effective at collecting and analysing malware from illegal IPTV technologies, it does have limitations. One limitation of the IITMAF software is that the time to complete the analysis is high, as multiple URLs and files are submitted to dynamic analysis, which can take time. In addition to this, the iterative approach employed in the methodology extends the analysis time even further. However, dynamic analysis and URL collection limits can be set to shorten this duration, providing configurability for the IITMAF. The depth of the recursion can be set using the internal parameters of the IITMAF. For this reason, per comparison, we have focused on the correct identification of the URL and IPTV resource.

Another limitation of the framework is that it provides limited analysis results for archive and Android-specific files, as they cannot be executed in the default Windows sandbox. Despite any limitations, the IITMAF focuses chiefly on the analysis of illicit IPTV websites, but we plan to address these limitations in the future work section. Additionally, our solution presents a guideline for the digital investigation of malicious files for the illegal IPTV domain rather than constituting a real-time application for stopping users from installing these applications, as the installation and access in most cases are conducted by the user themself without understanding/knowing the malicious intent behind. For the real-time application of the IITMAF, the signatures that are generated with the in-depth URL analysis would include the signatures that are branching from the suspicious/malicious URL itself. These in turn can be fed into IPS/IDS systems or Unified Threat Management (UTM) systems to cover a wider area of the neighbouring URLs where, without the analysis provided by the IITMAF, such systems can only block the front-facing URL content and the dynamically loaded content, and redirections would be omitted. Similarly, without the IITMAF, this analysis on the neighbouring URLs and the dynamic content would have to be performed by the analyst otherwise.

Overall, the IITMAF provides a successful solution to the defined problem, providing cybersecurity professionals with both manual and automatic methodologies for identifying malware threats in the illicit IPTV ecosystem in addition to an automated solution for detecting, collecting, and analysing malware from illegal IPTV technologies.

The IITMAF primarily aims to analyse illicit IPTV websites with its depth-first URL collection results. This functionality reveals possible external malvertising domains for an illicit website, including the loaded dynamic content. Although the URL and file analysis functionality meets the core requirements and detected a greater number of URLs as malicious than VirusTotal in this evaluation experiment, it has two minor limitations. One of these limitations is that for the submitted research sample in this evaluation experiment, only 4 out of the 60 URLs analysed had YARA rule matches indicating malicious capabilities. Nonetheless, 31 of the URLs had YARA rule matches for base64 encoded functions, implying that the static analysis functionality works properly. Additionally, one of the URLs pointing to an executable file had multiple YARA matches suggesting that it was malicious, as shown in Figure 11. This indicates that the signature-based malware detection functionality for IITMAF using YARA rules is still relevant and can detect malicious capabilities.

The other limitation of the IITMAF analysis functionality is that it was unable to conduct dynamic analysis for ZIP files, as Hybrid Analysis does not automatically extract files from them. This suggests that the IITMAF has limitations when analysing illicit IPTV add-ons, as they are frequently distributed using ZIP files.

```
{
 "url": "http://download.findmysoft.com/2014/05/19/ROX-Player_1.480.msi",
 "iptv_analysis_report": {
  "static_analysis": [
   {
    "url": "http://download.findmysoft.com/2014/05/19/ROX-Player_1.480.msi",
    "signatures": {
     "yara_file_rule_matches": [
      {
       "url": "http://download.findmysoft.com/2014/05/19/ROX-Player_1.480.msi",
       "matches": [
        "maldoc_structured_exception_handling",
        "network_http",
        "escalate_priv",
        "win_registry",
        "win_token",
        "win_files_operation",
        "Str_Win32_Winsock2_Library",
        "Str_Win32_Wininet_Library",
        "Str_Win32_Internet_API",
        "Str_Win32_Http_API"
       ]
      }
     ],
```


Figure 11. IITMAF report showing matched YARA rules for a URL.

In summary, the automated URL and file analysis functions of the IITMAF are effective at detecting malware and supplying detailed information about a file or URL's capabilities and behaviour. While there are some minor limitations, the analysis functionality meets the key requirements set and passes all the major unit tests.

In the future, we intend to improve the IITMAF by implementing additional features to the automated solution. One of these features would be downloading files from scraped webpage URLs depending on if a URL HTTP request header's content type relates to a non-webpage file. This would ensure that non-webpage files referenced by URLs that do not identify a file extension in the URL path are downloaded. Additional functionality to be developed would be mechanisms to bypass website CAPTCHAs, providing more accurate analysis results of malicious activity on illicit IPTV websites. Moreover, we plan to implement a Hybrid Analysis interface function for performing dynamic analysis on Android APK files, as many illicit IPTV technologies consist of Android applications that cannot be dynamically analysed in a standard Windows-based sandbox. Finally, as the Hybrid Analysis API is unable to automatically unpack archive files, we aim to implement functionality that automatically unpacks downloaded archive files and submits the contents for analysis, as illicit IPTV software add-ons can be distributed in an archive format.

Author Contributions: Conceptualization, A.L. and C.Y.; Investigation, A.L.; Methodology, A.L.; Project administration, V.K.; Software, A.L.; Supervision, C.Y. and V.K.; Validation, A.L., I.C., C.Y. and J.H.-B.; Writing—original draft, A.L.; Writing—review and editing, I.C. and J.H.-B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Digital Citizens Allience. How Digital Platforms Are Being Overrun by Bad Actors and How the Internet Community Can Beat Them at Their Own Game. 2017. Available online: https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Trouble-in-Our%20Digital-Midst%20Report-June-2017.pdf (accessed on 25 August 2023).
2. Digital Citizens Allience. Fishing in the Piracy Stream: How Dark Web of Entertainment Is Consumers to Harm. 2019. Available online: https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf (accessed on 25 August 2023).

3. Hsiao, L.; Ayers, H. The Price of Free Illegal Live Streaming Services. *arXiv* **2019**, arXiv:1901.00579.
4. Watters, P. A Systematic Approach to Measuring Advertising Transparency Online: An Australian Case Study. *SSRN Electron. J.* **2013**. [CrossRef]
5. Simpson, W.; Greenfield, H. What Is Internet Protocol, and Why Use It for Video? In *IPTV and Internet Video*; Elsevier: Amsterdam, The Netherlands, 2009; pp. 1–14.
6. Sandvine Subscription Television Piracy Sandvine Global Internet Phenomena Spotlight. Case Study 2 Global Internet Phenomena Spotlight. 2017. Available online: https://www.sandvine.com/hubfs/downloads/reports/internet-phenomena/sandvine-spotlight-subscription-television-piracy.pdf (accessed on 25 August 2023).
7. Pandey, P.; Aliapoulios, M.; McCoy, D. Iniquitous Cord-Cutting: An Analysis of Infringing IPTV Services. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden, 17–19 June 2019; pp. 423–432.
8. Intellectual Property Office. UK Government Response to the Call for Views Regarding Illicit IPTV Streaming Devices. 2018. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/750177/Gov-Response-call-for-views-Illicit-IPTV.pdf (accessed on 25 August 2023).
9. EUIPO. Illegal Iptv in the European Union. 2019. Available online: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_Ex_Summ_en.pdf (accessed on 25 August 2023).
10. Warrior, M.A.; Xiao, Y.; Varvello, M.; Kuzmanovic, A. De-Kodi: Understanding the Kodi Ecosystem. In Proceedings of the Web Conference 2020, Taipei, Taiwan, 20–24 April 2020; ACM: New York, NY, USA, 2020; pp. 1171–1181.
11. Dabral, S.; Agarwal, A.; Mahajan, M.; Kumar, S. Malicious PDF Files Detection Using Structural and Javascript Based Features. In Proceedings of the Communications in Computer and Information Science, New Delhi, India, 13 May 2017; Springer: Singapore, 2017; Volume 750, pp. 137–147.
12. Aljabri, M.; Altamimi, H.S.; Albelali, S.A.; Al-Harbi, M.; Alhuraib, H.T.; Alotaibi, N.K.; Alahmadi, A.A.; AlHaidari, F.; Mohammad, R.M.A.; Salah, K. Detecting Malicious URLs Using Machine Learning Techniques: Review and Research Directions. *IEEE Access* **2022**, *10*, 121395–121417. [CrossRef]
13. Samtani, S.; Chinn, K.; Larson, C.; Chen, H. AZSecure Hacker Assets Portal: Cyber Threat Intelligence and Malware Analysis. In Proceedings of the IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data, ISI 2016, Tucson, AZ, USA, 28–30 September 2016; pp. 19–24. [CrossRef]
14. Piplai, A.; Mittal, S.; Abdelsalam, M.; Gupta, M.; Joshi, A.; Finin, T. Knowledge Enrichment by Fusing Representations for Malware Threat Intelligence and Behavior. In Proceedings of the 2020 IEEE International Conference on Intelligence and Security Informatics, ISI 2020, Arlington, VA, USA, 9–10 November 2020. [CrossRef]
15. Miles, C.; Lakhotia, A.; Ledoux, C.; Newsom, A.; Notani, V. VirusBattle: State-of-the-Art Malware Analysis for Better Cyber Threat Intelligence. In Proceedings of the 7th International Symposium on Resilient Control Systems, ISRCS 2014, Denver, CO, USA, 19–21 August 2014. [CrossRef]
16. Tan, H.; Chandramohan, M.; Cifuentes, C.; Bai, G.; Ko, R.K.L. ColdPress: An Extensible Malware Analysis Platform for Threat Intelligence. *arXiv* **2021**, arXiv:2103.07012.
17. EUIPO. Identification and Analysis of Malware on Selected Suspected Copyright-Infringing Websites. 2018. Available online: https://euipo.europa.eu/knowledge/course/view.php?id=3395 (accessed on 25 August 2023).
18. Theocharidou, M.; Malatras, A.; Lella, I.; Tsekmezoglou, E. *ENISA Threat Landscape 2021*; European Union Agency for Cybersecurity: Attiki, Greece, 2021.
19. Khushali, V. A Review on Fileless Malware Analysis Techniques. *Int. J. Eng. Res.* **2020**, *9*, 46–49. [CrossRef]
20. Saad, S.; Mahmood, F.; Briguglio, W.; Elmiligi, H. JSLess: A Tale of a Fileless Javascript Memory-Resident Malware. In *Information Security Practice and Experience—ISPEC 2019*; Lecture Notes in Computer Science including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics; Springer: Cham, Switzerland, 2019; Volume 11879, pp. 113–131. [CrossRef]
21. Kara, I. Fileless Malware Threats: Recent Advances, Analysis Approach through Memory Forensics and Research Challenges. *Expert Syst. Appl.* **2023**, *214*, 119133. [CrossRef]
22. Ponemon Institute. The Third Annual Study on the State of Endpoint Security Risk. 2020. Available online: https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf (accessed on 25 August 2023).
23. Yucel, C.; Chalkias, I.; Mallis, D.; Karagiannis, E.; Cetinkaya, D.; Katos, V. On the Assessment of Completeness and Timeliness of Actionable Cyber Threat Intelligence Artefacts. In Proceedings of the Multimedia Communications, Services and Security: 10th International Conference, MCSS 2020, Kraków, Poland, 8–9 October 2020; pp. 51–66.
24. Xing, X.; Meng, W.; Lee, B.; Weinsberg, U.; Sheth, A.; Perdisci, R.; Lee, W. Understanding Malvertising Through Ad-Injecting Browser Extensions. In Proceedings of the 24th International Conference on World Wide Web, International World Wide Web Conferences Steering Committee, Geneva, Switzerland, 18 May 2015; pp. 1286–1295.
25. Sudhakar; Kumar, S. An Emerging Threat Fileless Malware: A Survey and Research Challenges. *Cybersecurity* **2020**, *3*, 1. [CrossRef]
26. Sanjay, B.N.; Rakshith, D.C.; Akash, R.B.; Hegde, V.V. An Approach to Detect Fileless Malware and Defend Its Evasive Mechanisms. In Proceedings of the 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), Bengaluru, India, 20–22 December 2018; pp. 234–239.

27. Abad, S.; Gholamy, H.; Aslani, M. Classification of Malicious URLs Using Machine Learning. *Sensors* **2023**, *23*, 7760. [CrossRef] [PubMed]
28. Mahesh; Ananth; Dheepthi. Using Machine Learning to Detect and Classify URLs: A Phishing Detection Approach. In Proceedings of the 2023 4th International Conference on Electronics and Sustainable Communication Systems, ICESC 2023—Proceedings, Coimbatore, India, 6–8 June 2023; pp. 1285–1291.
29. Difaizi, T.Z.; Camille, O.P.-W.L.; Benhura, T.C.; Gupta, G. URL Based Malicious Activity Detection Using Machine Learning. In Proceedings of the 2023 International Conference on Disruptive Technologies (ICDT), Greater Noida, India, 11–12 May 2023; pp. 414–418.
30. Ghaleb, F.A.; Alsaedi, M.; Saeed, F.; Ahmad, J.; Alasli, M. Cyber Threat Intelligence-Based Malicious URL Detection Model Using Ensemble Learning. *Sensors* **2022**, *22*, 3373. [CrossRef] [PubMed]
31. Rafsanjani, A.S.; Kamaruddin, N.B.; Rusli, H.M.; Dabbagh, M. QsecR: Secure QR Code Scanner According to a Novel Malicious URL Detection Framework. *IEEE Access* **2023**, *11*, 92523–92539. [CrossRef]
32. Sheppard, J. Cloud Investigations of Illegal IPTV Networks. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1942–1947.
33. Conti, M.; Dargahi, T.; Dehghantanha, A. Cyber Threat Intelligence: Challenges and Opportunities. In *Advances in Information Security*; Springer: Cham, Switzerland, 2018; Volume 70, pp. 1–6. [CrossRef]